IP Considerations Guide
For the IT Professional

CRESTRON®

Contents

Introduction

What is a Control System? 1
Why is it on my Network? 1
Proven and Trusted 1

Planning a Network with Crestron Devices

Isolate The Network 2
VLAN Configuration 2
Listen Ports 3
Connect Ports 4
IP Addressing 4
IPv6 4
Hostnames/Domain Names 4

Security

Security Setup 5
Firewall Setup / Communication Across Multiple VLANs 5
DigitalMedia Certified Designers and Engineers 6

DigitalMedia™ Network Considerations

DigitalMedia System Topology 6
DHCP Mode 7
Static Mode 8
DM-MD8X8 and DM-MD16X16 IP Architecture 8
Static Mode: DM-MD32X32 Architecture 10
Static Mode: DM-MD6X1 Architecture 10
IP Addressing Recommendations For Enterprise Network Installations 10
Rapid Spanning Tree Protocol (RSTP) 12
Best Practices for Managed Networks with Spanning Tree 12

Introduction

This guide is intended to outline the requirements, best practices and preferred methods of implementing Crestron devices on enterprise level networks. Focused on the concerns of the IT professional, Crestron is dedicated to providing the most accurate and pertinent information. If, after reading this document, you still have concerns about deploying Crestron devices on your network, please contact True Blue Support at 1-888-CRESTRON.

What is a Control System?

A control system is an appliance grade network-based device designed to control disparate devices and link them together over an IP network. It issues commands and gathers data to and from other devices based on user driven and automated events. Typically driving classroom and boardroom AV systems, a control system turns on the display and sets the correct input based on the press of a button on a touch screen, remote control or button panel (keypad). Control systems can even interface with the lighting and HVAC systems so when “PC” is selected, the lights dim to an appropriate level for viewing computer images.

The power behind Crestron control systems is the ability to custom program or configure them. Any single button press or collection of data can trigger any other number of events. The possibilities are truly endless.

Why is it on my Network?

Traditionally control systems have interfaced with devices via IR, RS-232, closed contacts and variable voltage. The natural progression over the past years has moved toward IP-based communication. Many devices have implemented IP protocols for control, monitoring and management mainly because IP is more common and cost effective to integrate.

Crestron systems were the first control systems to implement IP communication almost 15 years ago. Today, Crestron offers some of the most advanced IP devices in the AV and lighting control industry. Crestron systems can be controlled, maintained, and monitored from anywhere there’s an Internet connection. This greatly enhances the ability to update and troubleshoot systems without having to be physically on site.

Proven and Trusted

With installations in facilities of some of the technology leaders of the world like Microsoft® and Cisco®, Crestron control systems are suited for the most mission-critical and secure environments. After following the guidelines in this document, you can rest assured that Crestron devices will pleasantly coexist on your network.

Planning a Network with Crestron Devices

Before deploying a Crestron system on any network, it is important to consider the guidelines defined in the following sections. While there are many ways of configuring enterprise networks, these best practices have been found to be the most efficient and successful for Crestron devices.

Isolate The Network

Crestron devices should exist on a network separate from other device traffic. Other network activity can impact the response time of Crestron devices and disrupt the user experience.

Unlike most any other application communicating over your LAN/WAN, Crestron users expect instant control and feedback. To ensure constant connection and accurate feedback, proprietary Crestron control communications uses a heartbeat packet. Loss of round trip heartbeat packets indicate unreliable connections. This strict connectivity requirement ensures user confidence but is very latency sensitive.

Crestron recommends setting up all Crestron devices on a dedicated (Crestron only) VLAN so that unnecessary broadcast traffic does not interfere with the time sensitive packets between Crestron devices.

Deploying Crestron devices on a dedicated VLAN also enables you to provide network access control to them (in addition to username/password authentication, available on Crestron control systems).

VLAN Configuration

Whenever possible, all Crestron devices should be separated into their own VLAN. This will allow smoother operation of the control network and help manage the infrastructure—resulting in an overall better user experience.

The following steps should be taken to ensure that Crestron devices can be managed effectively:

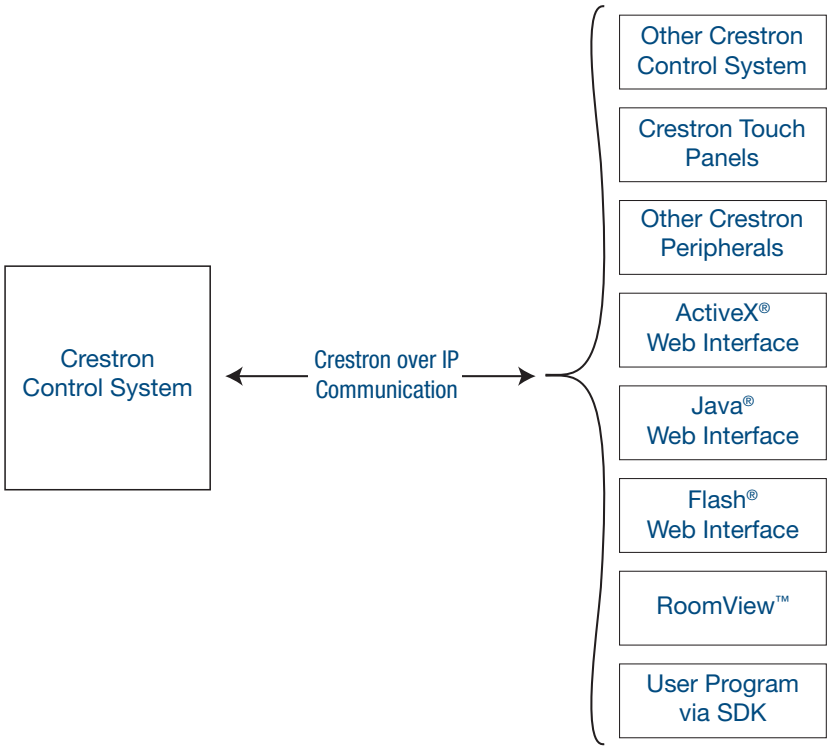
- If Crestron devices reside on multiple VLANs, static routes should be set up between VLANs on a router.
- DHCP requests should be forwarded to the appropriate VLAN with a DHCP server.
- Crestron ports should not be blocked for proper operation. A list of commonly used Crestron ports is available on page 3. For detailed information regarding what port numbers are required, please consult the appropriate device manual.
- Some devices allow for streaming media content from the Internet. These devices should be allowed to connect to the Internet if streaming is desired.

Listen Ports

A Crestron control system will listen to the following set of default ports (not all ports are turned on by default; consult product manual for more details):

Port	Protocol	Service	Notes
23	TCP	Telnet	
80	TCP	Web access	for user program interface and setup pages
161	UDP	SNMP	
443	TCP	Web access	active with SSL enabled
41794	TCP/UDP	Crestron over IP	Proprietary Crestron control communications
41795	TCP	Crestron console	Requires proprietary management tool
41796	TCP	Crestron over IP	active with SSL enabled
41797	TCP	Crestron console	active with SSL enabled

Diagram 1.1 - Crestron over IP Communications



The user program can add multiple listeners to the Crestron Control system. First, we recommend performing a security scan on the Control system without a program. Then, test with a program. This way it is easily determined if any security breaches are created by the program loaded in the control system.

Connect Ports

A Crestron control system will connect to the following set of default ports (not all ports are turned on by default; consult product manual for more details):

Port	Protocol	Service	Notes
25	TCP	SMTP	Only if enabled in control program
42	TCP/UDP	WINS Access	
53	UDP	DNS Access	
67/68	UDP	DHCP Configuration	
161/162	UDP	SNMP	
41794	TCP/UDP	Crestron over IP	Proprietary Crestron control communications
41796	TCP	Crestron over IP	active with SSL enabled

IP Addressing

In general, best practices are to assign Crestron devices static IP addresses. Communication amongst Crestron devices relies on IP addresses remaining the same. In large corporate or university environments, static or reserved DHCP is recommended to aid in managing devices.

In certain cases, like with DigitalMedia products, static mode may be preferred over DHCP. Please see “DigitalMedia™ Network Considerations” on page 6 for more information.

IPv6

All Crestron control systems can exist on an IPv6 network. For a list of Ethernet compatible control systems, see Appendix A on page 14.

Hostnames/Domain Names

Crestron best practices are to configure DNS and DHCP servers to allow hostnames to resolve via option 81 and option 12.

Security

The following security information is centered around Crestron control systems. For a list of control systems, see Appendix A on page 14.

Security Setup

Always define an administrator password – this guarantees that only authorized personnel can make changes to the configuration of Crestron equipment.

Enable SSL – to ensure that passwords are not sent clear-text over the network.

Have the Crestron programmer add passwords/passcodes to those sections of the user program that are related to configuration of third-party devices.

Firewall Setup / Communication Across Multiple VLANs

Crestron systems can be controlled remotely. For example, an iPad® running Crestron Mobile Pro® G on a 3G cellular network can send commands to the control system to adjusts the lights. In another scenario, a centrally located RoomView™ server requires communication across multiple networks in order to communicate with all rooms.

These applications require the following ports to have access to the outside network:

Port	Protocol	Service	Notes
80	TCP	Web server	Web pages can also be hosted via IIS or other corporate web server
443	TCP	Web server	For secure SSL access
41794	TCP	Crestron over IP	Proprietary Crestron control communications

Additionally, Crestron control systems can be managed from any IP address locally or remotely. Programs and firmware can be updated; diagnostic tests can be performed. For this communication, enable the following:

Port	Protocol	Service	Notes
41795	TCP	Crestron over IP	Use if SSL is disabled
41797	TCP	Crestron over IP	Use if SSL is disabled

DigitalMedia™ Network Considerations

It is important to know that most Crestron DigitalMedia (DM) devices are Ethernet devices. Ethernet traffic due to DigitalMedia devices is relatively low. The custom control system program that ties together the DM system will dictate how much bandwidth is needed.

DigitalMedia Certified Designers and Engineers

Every Crestron DigitalMedia system should be designed by a DigitalMedia Certified Designer (DMC-D) and commissioned by a DigitalMedia Certified Engineer (DMC-E). If you are unaware of a DMC-D or -E being involved with the deployment of the DM system on your campus, please contact you system installer.

Only Crestron certified engineers ensure that your system is properly installed and configured to Crestron standards. The information in this guide is intended to explain basic DM IP addressing considerations. Consult with your DMC-E if you have questions.

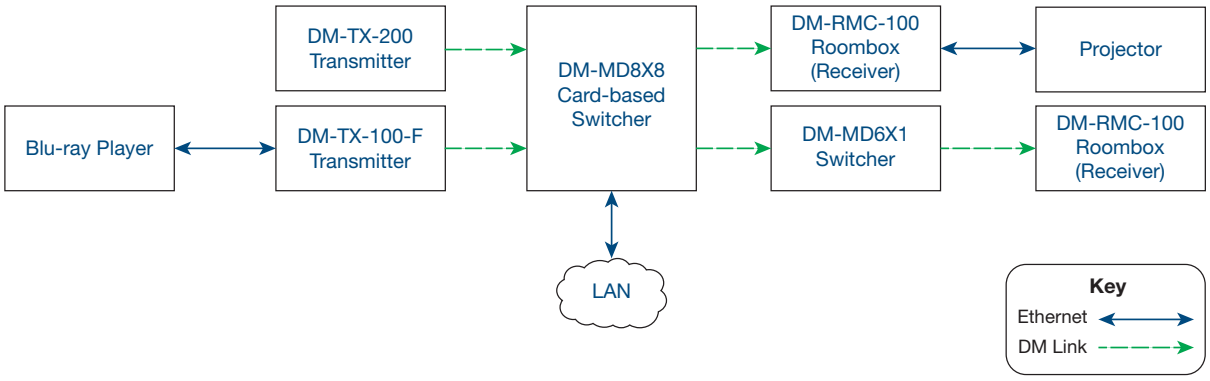
DigitalMedia System Topology

Each DigitalMedia link (connection between two DM devices) carries Ethernet embedded inside so that no additional wiring is needed to provide network connectivity for third party Ethernet products installed at the endpoints. Interconnected DM devices only need a single point (typically the main switcher) to be connected to the LAN in order to provide Ethernet to all devices in the system. To facilitate this, Crestron DM devices have integrated managed Ethernet switches and an exposed Ethernet port.

NOTE: A DM endpoint refers to any DM transmitter or roombox (receiver).

In the below scenario, Ethernet connectivity is provided to all DM devices and third party devices from the single LAN connection at the DM-MD8X8. This eliminates the need to run extra wiring to each location to provide Ethernet connectivity.

Diagram 3.1 - DigitalMedia Ethernet Connectivity



The main Ethernet uplink to a DM system occurs at the DigitalMedia switcher. The following switchers have 10/100/1000BaseT auto-negotiating uplink ports:

- DM-MD8X8, DM-MD16X16, DM-MD32X32

The following switchers have 10BaseT/100BaseTX auto-negotiating uplink ports:

- DM-MD6X1

Other devices in the DM family contain 10BaseT/100BaseTX auto-negotiating Ethernet ports.

Remember, DigitalMedia devices create a flat network that contains only switches—no DHCP servers or routers.

DHCP Mode

When the DM switcher is set to DHCP mode, all (addressable) cards and endpoints will also be set to DHCP mode. Each of these DigitalMedia devices will receive an IP address from the external DHCP server located on the network.

NOTE: When using DM 8G products (part numbers with the suffix "-C" or "-S"), DHCP mode will require more IP addresses than static mode. This is because a DM 8G input or output card can be assigned an IP address (unlike original DM CAT and fiber input and output cards—DMC-CAT(-DSP), DMC-F(-DSP), DMCO-"1", DMCO-"2").

Table 3.1 - Maximum Required IP Addresses in DHCP Mode

		DM-MD6X1	DM-MD8X8	DM-MD16X16	DM-MD32X32
# of IP Address	Switcher	1	1	1	1
	Transmitters	3	8	16	32
	Input Cards	0	8	16	32
	Output Boards	0	4	8	16
	Roomboxes (receivers)	1	8	16	32
	Total:	**5**	**29**	**57**	**113**

*An output card is made up of one or more output boards. Each board has at least two outputs.

Table 3.2 - IP Addressable DM Devices

Below is a full list of products that can be assigned IP addresses:

Switchers
DM-MD6X1
DM-MD8X8
DM-MD16X16
DM-MD32X32

Input Cards
DMC-HD
DMC-HD-DSP
DMC-DVI
DMC-SDI
DMC-C*
DMC-C-DSP*
DMC-S*
DMC-S-DSP*
*Require IP address only when in DHCP mode.

Output Cards
DMCO-"4"*
DMCO-"5"*

Output card model numbers are constructed with a series of numbers (either 2- or 4-digit)..

*Require IP address only when in DHCP mode.

Transmitters
DM-TX-100
DM-TX-100-F
DM-TX-200
DM-TX-201-C
DM-TX-201-S
DM-TX-300N
DM-TX-300N-F
DM-TX-200-2G
DM-TX-400-3G

Receivers/ Roomboxes
DM-RMC-100
DM-RMC-100-1
DM-RMC-100-F
DM-RMC-100-C
DM-RMC-200-C
DM-RMC-100-S
DM-RMC-150-S

A comprehensive list of DM products can be found in Appendix B on page 15.

Addressable Device Number

An “addressable device number” refers to the physical location of a card or card/endpoint combination within a DM switcher. This term is used when explaining how a DM switcher assigns IP addresses when in static mode.

Static Mode

When a DM switcher is set to static IP mode, all cards and endpoints will also be set to static mode. To reduce the amount of time needed to configure the IP addresses, DM switchers will configure the addressing for any applicable DM device (transmitter, receiver, input/output card). In DM, this IP mode can be thought of as an “automatic” static mode. The switcher’s mode is set, and all connected devices are automatically configured. The IP addressing scheme is detailed below:

DM device’s IP address = the switcher’s IP address + the addressable device number

It is best to set aside an IP address range to accommodate an entire switcher:

Table 3.3 - Maximum Consumed IP Addresses in Static Mode

Switcher	Range of IP Addresses to Block (including switcher’s IP)	Maximum # of IP Addresses that will be used
DM-MD8X8	25	17
DM-MD16X16	33	33
DM-MD32X32	65	65
DM-MD6X1*	18	5

Depending on the DM system configuration, not all IP addresses in this “blocked out” range will be used.

**When more than one DM-MD6X1 is used on a network, the base IP addresses can be staggered in a way to maximize an IP address range. See Appendix C on page 16 for more information.*

NOTE: A DM switcher will never configure the IP information of another switcher, even if they are interconnected via DM.

DM-MD8X8 and DM-MD16X16 IP Architecture

Both the DM-MD8X8 and DM-MD16X16 share the same hardware architecture. Diagram 3.2 on page 9 shows a typical switcher layout. Sample IP addresses have been inserted to demonstrate the addressing scheme.

- Input cards utilize addressable device numbers 1-16
- Output cards utilize addressable device numbers 17-32
- A DM-MD8X8 doesn’t have addressable device numbers 9-16 or 25-32, but a DM-MD16X16 does
- “Automatic” static IP addressing on DM is done out-of-band and is not in any way a DHCP server.
    - › It is equivalent to assigning a static IP address to each device manually.

Diagram 3.2 - DM-MD8X8 and DM-MD16X16 Architecture

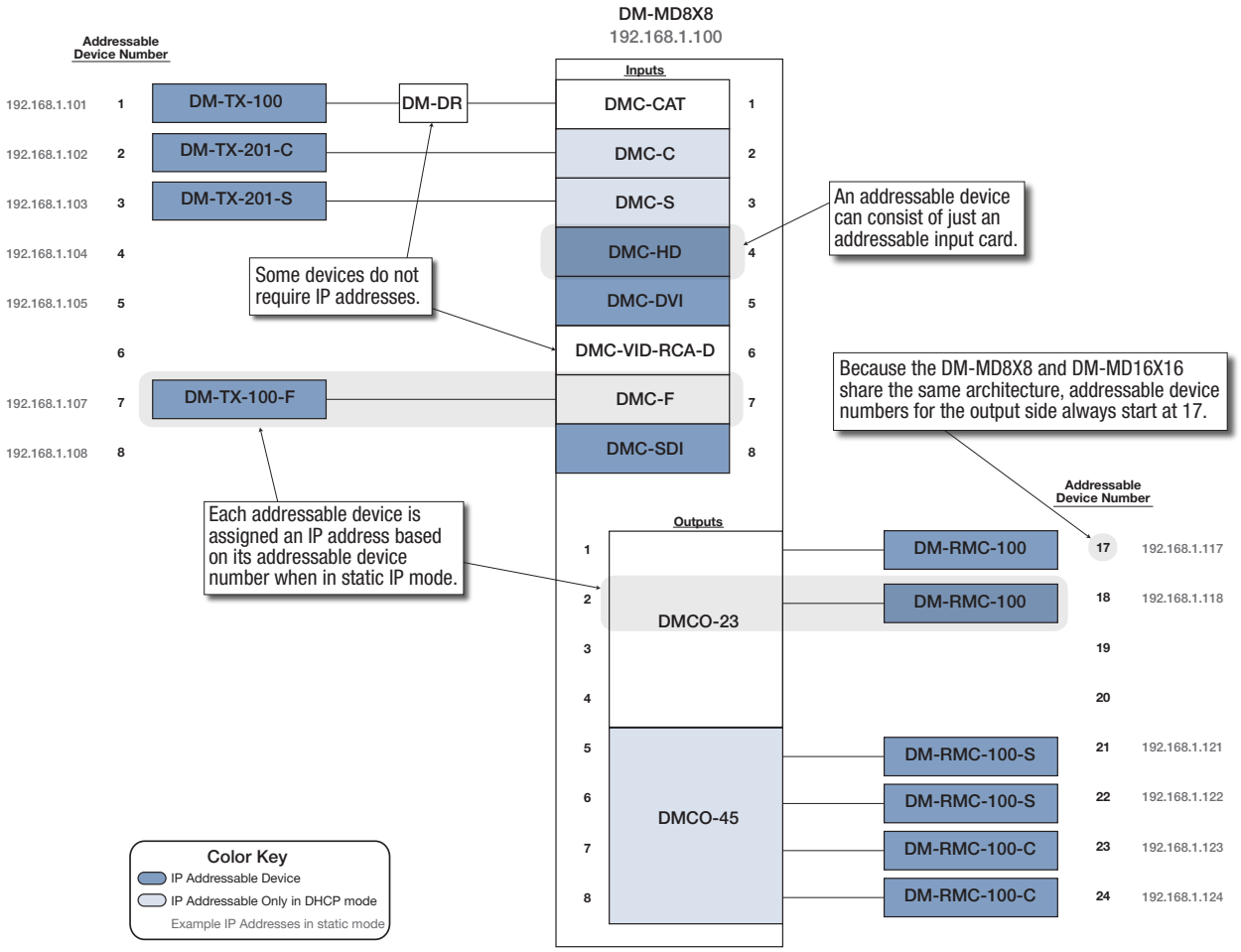
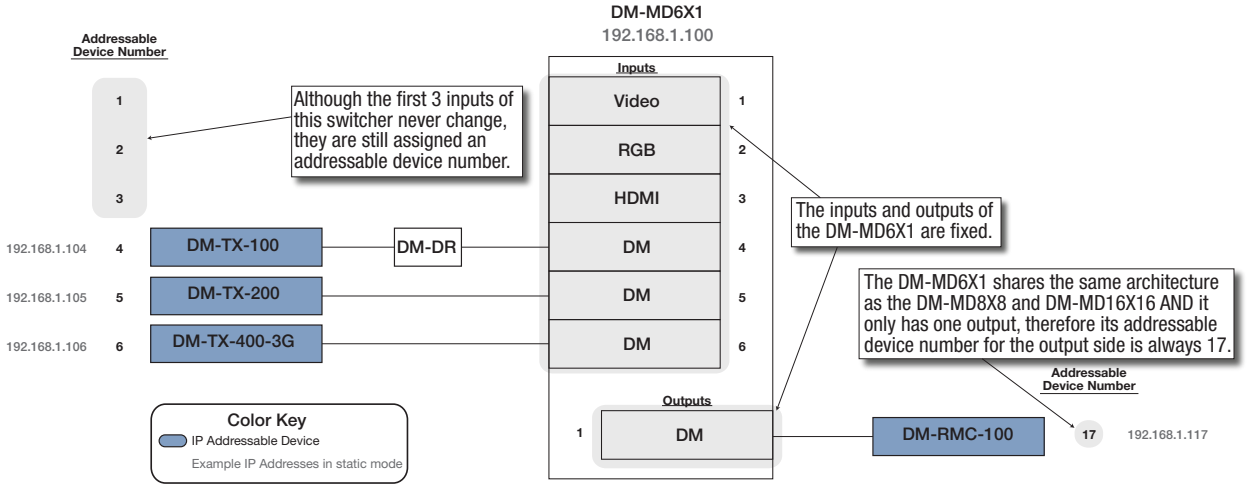


Diagram 3.3 - DM-MD6X1 Architecture



Static Mode: DM-MD32X32 Architecture

Diagram 3.5 on page 11 illustrates the architecture of a DM-MD32X32.

Similar to the DM-MD8X8 and DM-MD16X16 architecture, the DM-MD32X32 assigns IP addresses based on addressable device numbers:

- Input cards utilize addressable device numbers 1-32
- Output cards utilize addressable device numbers 33-64

NOTE: In static mode, a fully loaded DM-MD32X32 can consume up to 65 IP addresses. It is important to set the IP address of the switcher low enough so you don't run out of addresses within the subnet (i.e., don't set the IP address of a 32X32 higher than x.x.x.142 in a network with a subnet mask of 255.255.255.0).

Static Mode: DM-MD6X1 Architecture

Diagram 3.3 on page 9 illustrates the architecture of a DM-MD6X1.

Only five (5) IP addresses are needed for a maximum DM-MD6X1 system. The automatic static addressing scheme in this switcher is similar to that of the 8X8 and 16X16 switchers. To avoid any network address conflicts, it is best practice to block out the range of 17 IP addresses after the base IP of the DM-MD6X1. When multiple 6X1 switchers are deployed on a single network, the base IP addresses can be staggered in a way to maximize the address use in that range. See Appendix C on page 16 for more information.

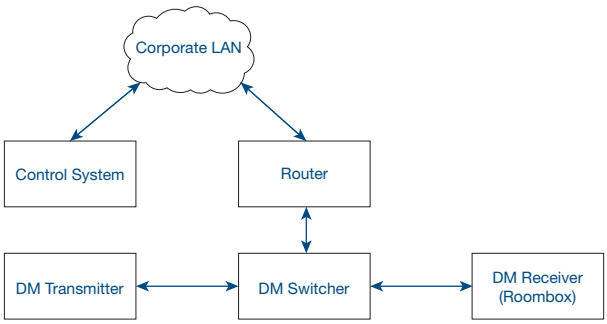
If there is a low overhead of IP addresses where this device is to be installed, use static (reserved) DHCP.

IP Addressing Recommendations For Enterprise Network Installations

In scenarios where a number of DM switchers must be managed on the same subnet, the preferred method is to set the DM switchers to DHCP mode. By doing this, you only need to request the number of IP addresses that are actually used by the devices instead of blocking out a larger IP address range. Static DHCP can assist with managing the DM device IP address allocation but it is not required for operation.

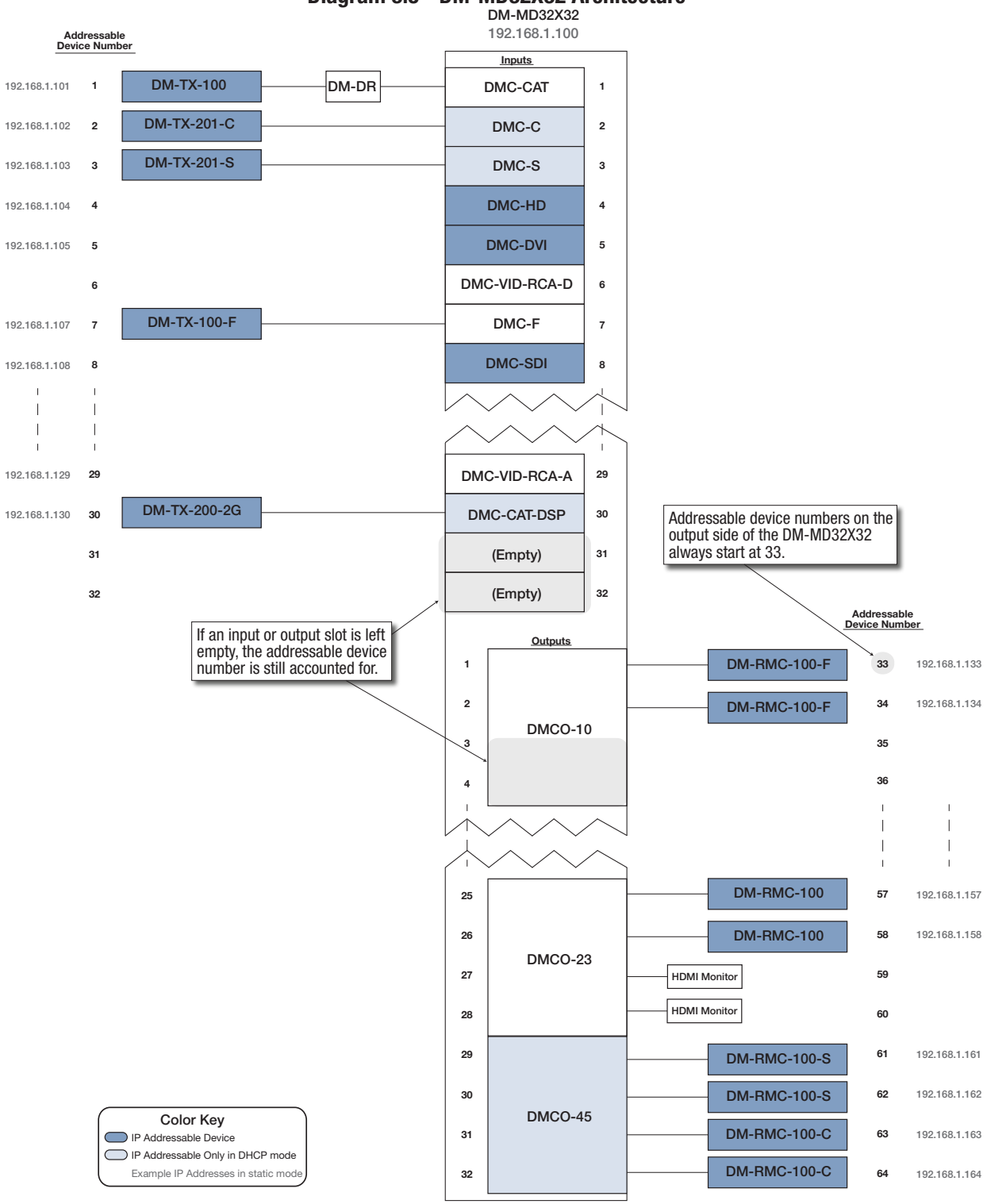
If your network is designed such that you cannot block out a range that large and you cannot request a large number of IP addresses from the DHCP server then it is best to install the DM switcher behind a separate network. See diagram below:

Diagram 3.4 - DigitalMedia Switcher Behind Separate Network



In this scenario the control system is not behind the router so it can be managed by RoomView and be made available for remote login.

Diagram 3.5 - DM-MD32X32 Architecture



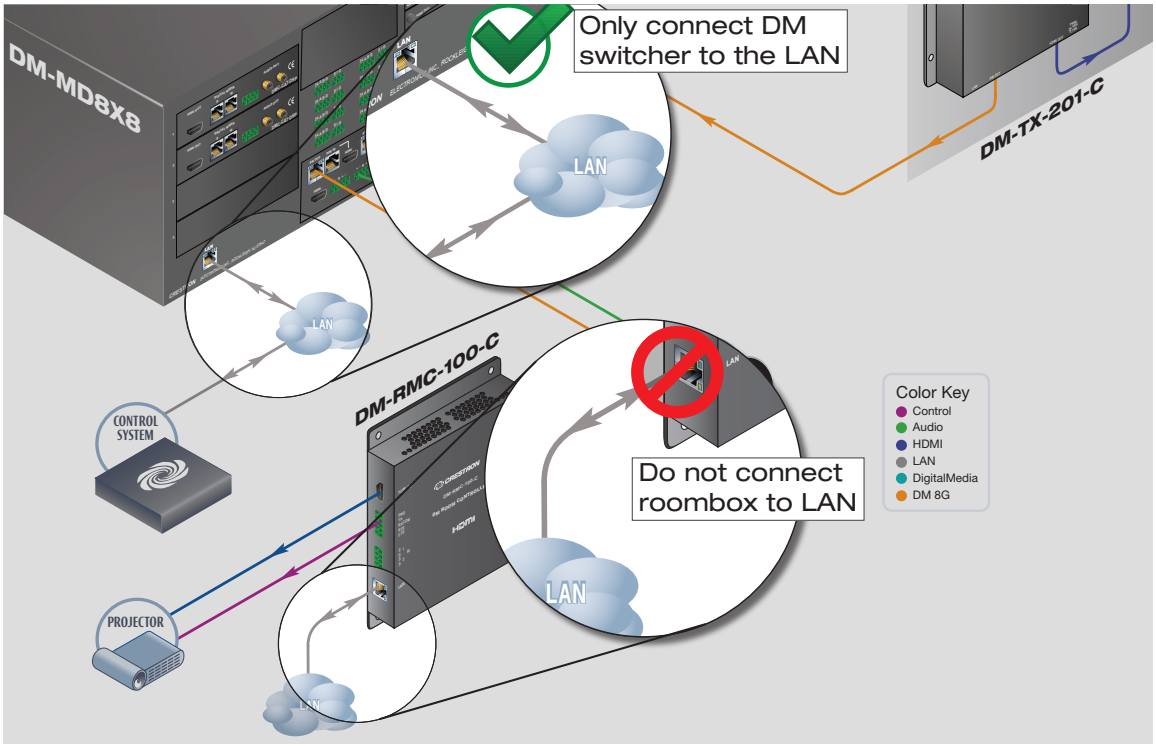
Rapid Spanning Tree Protocol (RSTP)

Because DigitalMedia devices embed Ethernet in every link, it is possible to create valid AV configurations that will create network loops – such as routing two AV signals from one switch to another switch. To eliminate any network looping problems, DigitalMedia products implement IEEE 802.1w Rapid Spanning Tree Protocol (RSTP).

You may notice that the DigitalMedia products transmit BPDUs per the RSTP specification. The DM products are given the lowest possible RSTP priority so that network traffic flows through the regular corporate LAN and loops are only broken inside of the DigitalMedia system.

By default, every DM device ships with RSTP turned on. If desired, it can be turned off.

Illustration 3.1 - Incorrect Network Wiring



Best Practices for Managed Networks with Spanning Tree

If you are using a router between the DigitalMedia system and the network, this section does not apply, as the router will completely segment the two networks. Using a router is a good solution for some customers who are unable to ensure that the below best practices can be implemented. Another solution is to disable RSTP on DigitalMedia products and manually break any loops. Contact Crestron Technical Support (1-888-CRESTRON) for assistance with this.

RSTP is a link layer (layer 2) network protocol that ensures a loop-free topology for any LAN. Very advanced users can find more information on RSTP in the Cisco whitepaper found on their website.

There is a more advanced version of RSTP called MSTP that supports multiple spanning trees on multiple VLANs. DigitalMedia implements RSTP, but not MSTP. If you are running MSTP on your network you should ensure that the network port that DigitalMedia is connected to only belongs to one VLAN. This is because RSTP ignores multiple VLAN trees maintained on the MSTP end.

Managed Ethernet switches can be configured to have “edge ports” which means that no Ethernet switches can be plugged into those ports. If you plug DigitalMedia into an edge port, the managed switch may shut the port down because the DigitalMedia device looks like a network switch. To avoid this, ensure that the switch ports are configured correctly where you are connecting DM products.

Appendix A - Crestron Control Systems with Ethernet

3-Series Control Systems

MC3
PMC3-XP
PMC3

2-Series Control Systems

PRO2*
AV2*
RACK2*
CP2E
MC2E
MP2E
QM-RMC
QM-RMCRX-BA
PAC2*
PAC2M
DIN-AP2
IPAC-GL1
PMC2
*Requires Ethernet Card

Devices with Integrated 2-Series Control Systems

MPC-M5
MPC-M10
MPC-M20
MPC-M25
MPC-M50
MPS-100
MPS-200
MPS-250
MPS-300
AADS
AADS-XM
AES
AMS
AMS-AIP

Ethernet Cards

C2ENET-1
C2ENET-2

Appendix B - DM Devices by Category

Integral Switchers
DM-MD6X1

Card-based Switchers
DM-MD8X8
DM-MD16X16
DM-MD32X32

Digital Video Input Cards
DMC-HD
DMC-HD-DSP
DMC-DVI
DMC-SDI

Analog Video Input Cards
DMC-VID-RCA-D*
DMC-VID-RCA-A*
DMC-VID-BNC*
DMC-VID4*

CAT/Fiber Input Cards
DMC-CAT*
DMC-CAT-DSP*
DMC-F*
DMC-F-DSP*

8G STP/Fiber Input Cards
DMC-C**
DMC-C-DSP**
DMC-S**
DMC-S-DSP**

CAT/Fiber Output Cards
DMCO-"1"*
DMCO-"2"*

HDMI Output Cards
DMCO-"3"*

8G STP/Fiber Output Cards
DMCO-"4"**
DMCO-"5"**

Output card model numbers are constructed with a series of numbers (either 2- or 4-digit). Each digit represents one output board.

Some examples of DMCO part names are: DMCO-11, DMCO-23, DMCO-2222, DMCO-5533

For a complete list of DMCO models, please refer to the Crestron website or click here.

CAT/Fiber Transmitters
DM-TX-100
DM-TX-100-F
DM-TX-200
DM-TX-300N
DM-TX-300N-F
DM-TX1-1G*
DM-TX-200-2G
DM-TX-400-3G

8G STP/Fiber Transmitters
DM-TX-201-C
DM-TX-201-S

CAT/Fiber Receivers/ Roomboxes
DM-RMC-100
DM-RMC-100-1
DM-RMC-100-F
DM-RX1-1G*

8G STP/Fiber Receivers/ Roomboxes
DM-RMC-100-C
DM-RMC-200-C
DM-RMC-100-S
DM-RMC-150-S

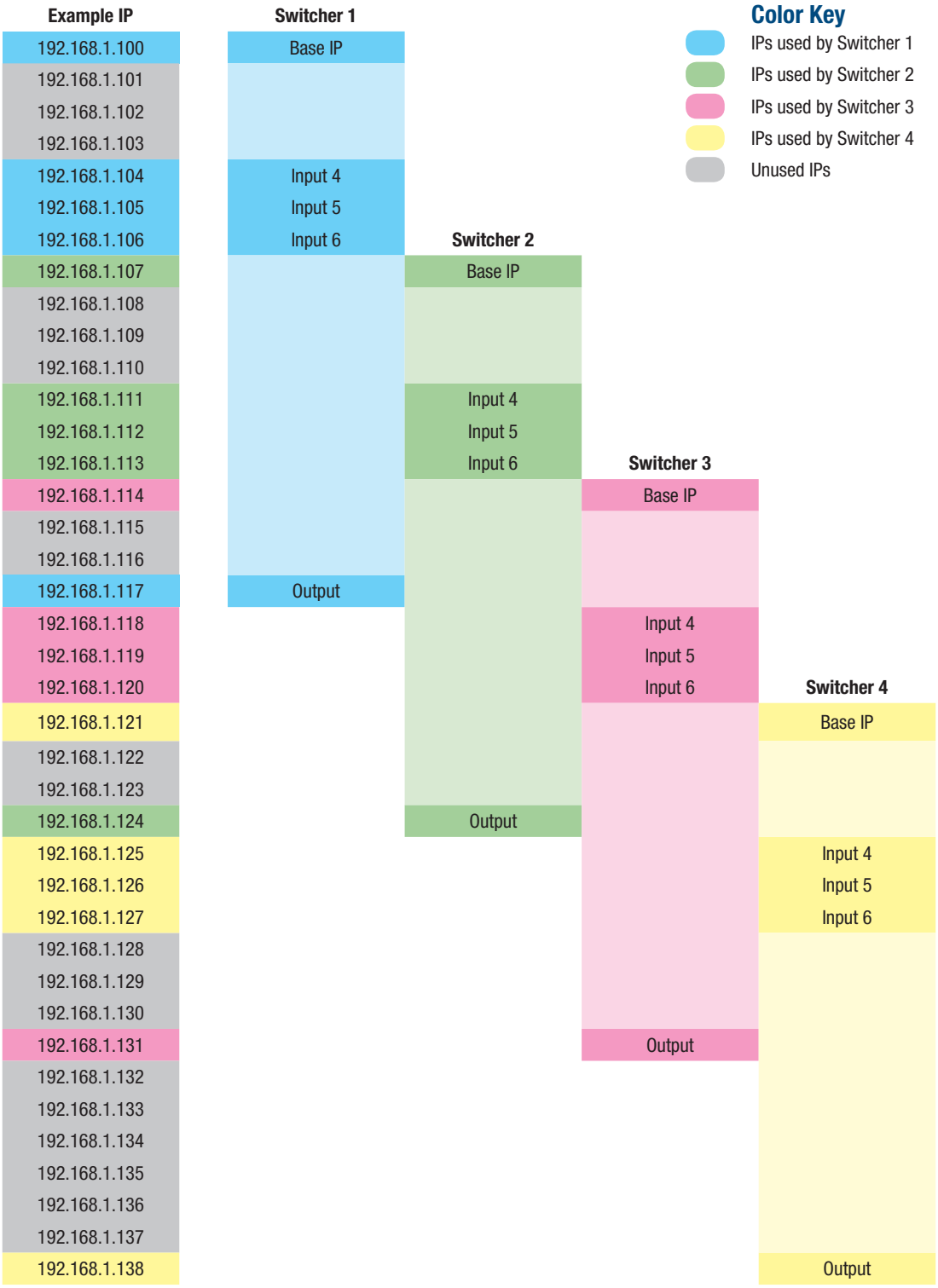
All DM devices listed consume an IP address except where noted.
*Can never consume an IP address
**Consumes IP address only when in DHCP mode

"CAT/Fiber" – refers to original DigitalMedia products that use original DM cable or two strands of multimode fiber.

"8G STP/Fiber" – refers to 8G DigitalMedia products that use a single STP DM 8G wire or a single strand of multimode fiber.

Appendix C - Staggered Base IP Addresses

In certain situations, like when multiple DM-MD6X1 switchers are deployed on the same network, the base IP address of the switchers can be staggered to maximize the range of IP addresses:



Crestron World Headquarters
15 Volvo Drive
Rockleigh, NJ 07647
800.237.2041
201.767.3400
Fax: 201.767.1903
crestron.com

Crestron International Headquarters
Oude Keerbergsebaan 2
2820
Rijmenam
Belgium
+32.15.50.99.50
Fax: +32.15.50.99.40
crestron.eu

Crestron Asia Headquarters
Room 2501, 25/F, Westin Centre
No. 26 Hung To Road
Kwun Tong
Hong Kong
+852.2341.2016
Video Ph: +852.2373.7530
Fax: +852.2344.0889
crestronasia.com

Crestron Latin America Headquarters
Blvd. Manuel Avila Camacho No 37-1A
Col. Lomas de Chapultepec
CP 11560 México DF
+55.5093.2160
Fax: +55.5093.2165
crestronlatin.com

Printed in USA Doc.4579A 2/11

Products manufactured in the United States.

Crestron, the Crestron logo, Crestron Mobile Pro, RoomView, and DigitalMedia are trademarks or registered trademarks of Crestron Electronics, Inc. in the United States, other countries or both. iPad is a trademark of Apple Inc., registered in the U.S. and other countries. Microsoft and ActiveX are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Cisco is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Adobe and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims proprietary interest in the marks and names of others.

©2011 Crestron Electronics, Inc.